 IAB

Central Intelligence Agency

Washington, D.C. 20505

OLL 84-1328/2
10 April 1984

MEMORANDUM FOR: Peter Sullivan
John Elliff
Ed Levine

STAT FROM: [redacted]
Chief, Legislation Division
Office of Legislative Liaison

SUBJECT: Delegation of GSA Authorities Provision in the Draft Fiscal Year 1985 Intelligence Authorization Bill

1. Enclosed at Tab A, per your request, is a draft guard force implementation plan prepared by the Office of Security. It should be noted that this plan was prepared prior to our discussions with the Office of Management and Budget and anticipates an assumption of this guard force function at all Agency facilities rather than the four buildings which have been presently identified. Also enclosed at Tab B is a clean copy of the procedures promulgated pursuant to Executive Order 12036 relating to the collection of information on United States persons which define the scope of physical security investigations.

2. With respect to your question as to whether GSA presently maintains security files on known terrorist or dangerous persons, our conversations with GSA indicate that GSA records in this respect are limited to the compilation of information concerning certain dangerous groups, and to reports on actual incidents involving threats to Federal property or personnel. We have confirmed that the Office of Security does not intend to seek the transfer of these files from GSA or to expand their collection activities in this regard following the delegation of these additional authorities.

STAT [redacted]

Enclosures

DISTRIBUTION:
Original - Each Addressee
1 - OLL Chrono
1 - LEG File: 85 Intel. Auth. Bill
1 - SWH Signer
1 - D/OLL
1 - DD/OLL
STAT 1 - [redacted] Liaison
SWH:csh (10 April 1984)

 7AB A

GUARD FORCE IMPLEMENTATION PLAN

GUARD FORCE IMPLEMENTATION PLAN

OPERATING CONCEPT

The new CIA guard force will function under the same operational concept now employed at CIA Headquarters STAT and NPIC. Essentially, operational control of security activities will continue to rest with the Security Duty Officer (SDO). Management, supervision, inspection, training, and other support will come from the command structure within the new Access Control Section (see Attachment I).

No changes are needed in the SDO and guard force operating procedures now in effect. However, guards will be closely supervised to insure strict conformance with written or oral commands.

The new guard force will operate with three permanent shifts. Personnel will work an eight and one half hour shift (8½) with a thirty (30) minute meal break and two fifteen (15) minute breaks. All basic CIA operating procedures and personnel policies will apply.

GUARD TASK FORCE

The Office of Security (OS) Guard Task Force has been created to support the OS implementation of a CIA staff employee guard force to replace the present GSA Federal Protective Staff guard force.

The Guard Task Force functions under the leadership of the Deputy Director of Security (DD/OS) and members will be responsible for resolving specific concerns in coordination with the Chief, Headquarters Security Branch (HSB). As the DD/OS's representative, C/HSB will act as overall project coordinator with primary responsibility for identification of concerns, objectives, and priorities. The task force will meet as necessary at the direction of DD/OS or at the recommendation of any member.

IMPLEMENTATION PLANS

The new CIA guard force project will be implemented according to the following plans:

RECORDS

Special effort will be paid to production and acquisition of historical records which clearly define the

DCI's intentions, concerns, objectives, and priorities for a CIA guard force.

NOTIFICATIONS

Action will be taken to make responsible DDA office directors, such as the Director of Personnel, clearly aware of requirements in support of this effort. Also, the general Agency population will be informed, via Headquarters notice, of intended guard force changes during the transition period.

REORGANIZATION

Very early during the first year of transition, HSB will reorganize internally which will elevate guard activities to the section level (see Attachment II). This reorganization will more clearly assign responsibilities by function and allow more availability of management support during creation of the new guard force. The Deputy Chief, HSB will be responsible for day-to-day management of Branch activities with special attention to the Access Control Section. The Chief, HSB will continue to concentrate on advance problem identification and solution.

SUPERVISORS

Guard force supervisors will be hired as soon as possible to support other tasks related to the creation of the guard force. As a general concept, major emphasis will be placed on applicant qualifications when selecting potential guard force supervisors. Quality will be favored over urgency. Preferably, persons with high potential will be recruited for junior supervisory positions with consideration for advancement to higher positions as Phase II and Phase III are accomplished.

PERSONNEL

PMCD concurrence on recommended slot levels will immediately be requested. The DCI's commitment to the success of this project will be highlighted to PMCD reviewers early on to prevent the possible need for lengthy appeals.

TERMS OF EMPLOYMENT for new guard force applicants would generally be similar to the standard staff employee three year trial period concept. Additionally, all applicants will be

asked to sign an agreement obligating them to a minimum of two years before eligibility to transfer to other Agency components. The agreement would also bind applicants to a strict guard code of conduct, performance, and dress. A concerned management concept will enforce strict compliance and actively seek employee termination as necessary.

RECRUITMENT of guard force applicants will be from all available sources with heavy emphasis on the outlying areas of Northern Virginia. OS representation will participate as much as possible in recruitment campaigns. At least 2 HSB managers will personally interview each local applicant. Out-of-town applicants will be telephonically interviewed by an HSB representative before being placed in process. These applicants will receive final interviews by at least two HSB managers during their visit to Headquarters for polygraphing. Processing for any undesirable candidates will be cancelled immediately. In all cases, final selection of applicants will be made by C/HSB.

EMPLOYMENT OF ON BOARD FPOs BY CIA will not be considered until a sufficient number of vacancies have been filled by new guards. FPO applicants will be considered on the record of their past work at CIA facilities. FPOs are not expected to resign their positions with FPS before applying for CIA employement. They will be required to undergo the same EOD personnel and security processing as other CIA applicants. FPOs with over one year FPS experience at CIA facilities can expect consideration for employment at the GS-6 level.

SECURITY PROCESSING

All security clearance processing for guard force applicants will be initiated at the highest priority level. Applicants will undergo a Pre-process interview before up-front polygraph examination. Background investigations will be scheduled on a 30 day expedite basis.

SPACE

No additional space will be required for a CIA guard force. The new force will assume that space now occupied by FPS. FPS space will be acquired pro-

portional to the per cent of slots assumed by CIA during the transitional period.

FINANCES

During the transition period, reimbursable payments to GSA will be adjusted quarterly according to the number of positions assumed by CIA. Adjustment to SLUC will not be of concern since charges for protection of federal property will be discontinued by GSA after October 1984. Since the Agency immediately assumes responsibility for any vacant FPO slots at the time the Delegation of Authority is signed, the Agency will thereafter be responsible for FPS overtime costs required to man these posts. CIA, of course, will not make next-quarter reimbursable payments to FPS for any vacant slots.

TRAINING

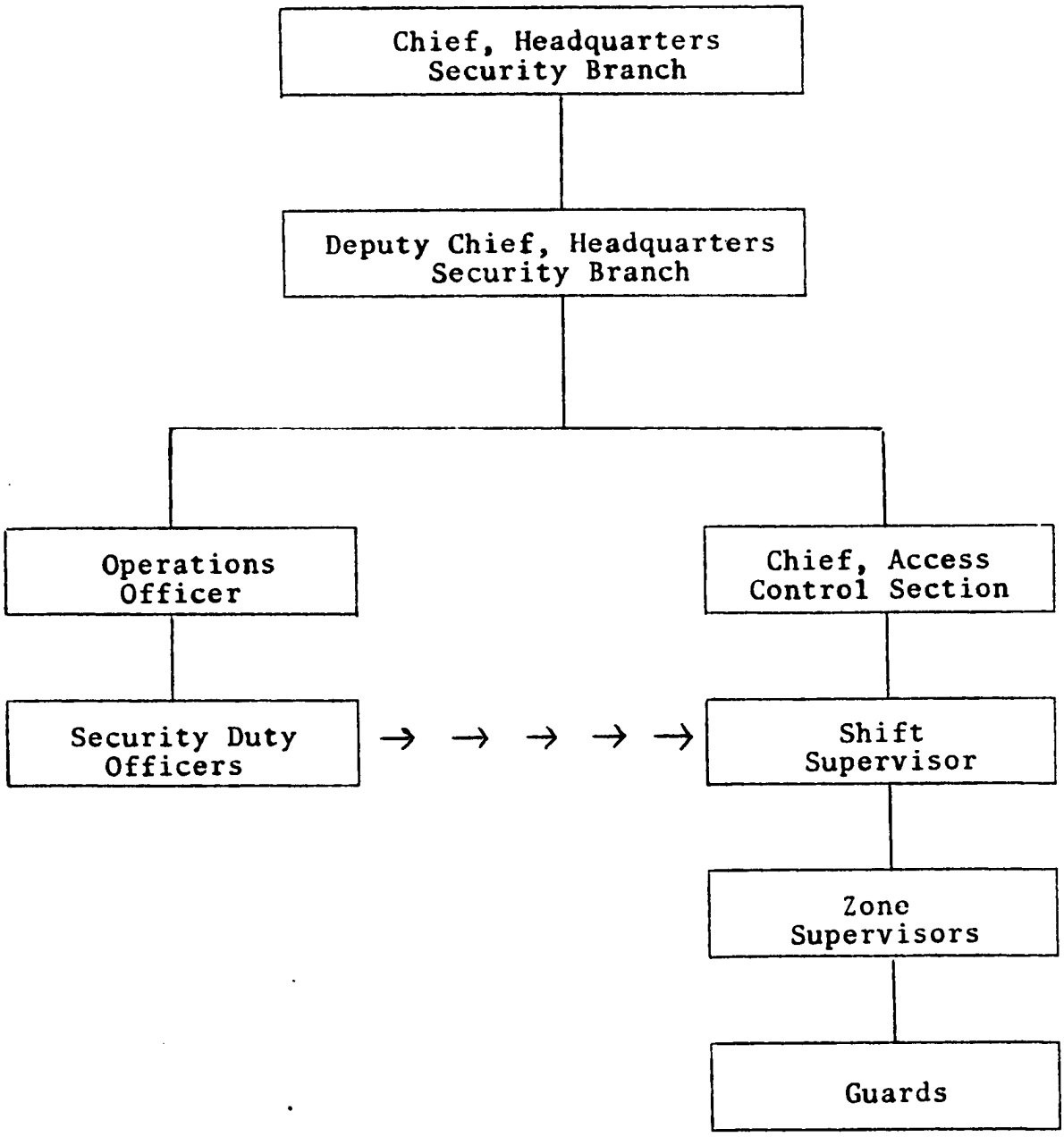
CIA will incorporate the best different types and styles of training for the new CIA guard force. Although use of weapons and resistance to forced intrusion will be addressed, the main thrust of training will center on identification with the Agency mission, access control and the OS "helping hand" philosophy. The objective of CIA guard training will be to produce a qualified,

courteous, presentable, and interested guard. To accomplish this goal, training outlines will be reviewed from all major federal guard and police academies and those applicable parts incorporated into the HSB guard training program.

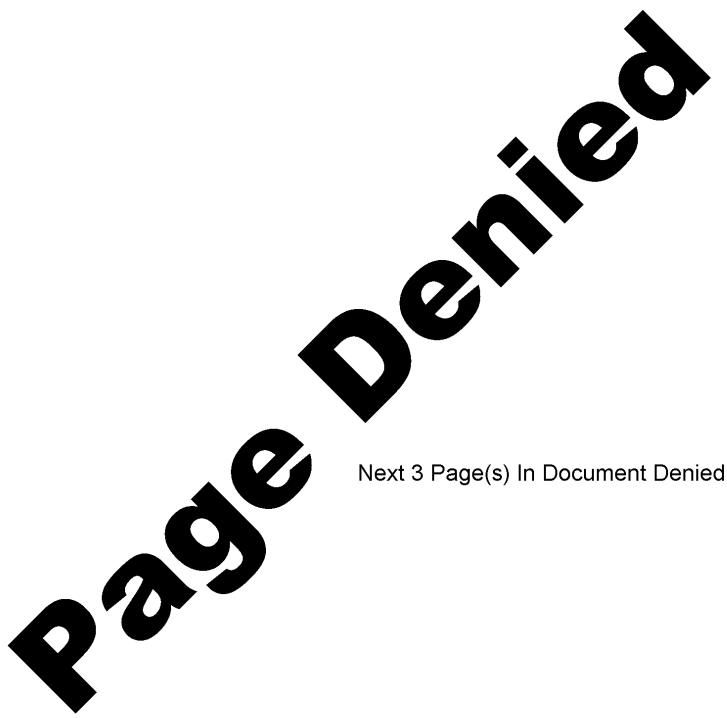
UNIFORMS

In addition to continuation of the two blazer (blue and tan colors) concept for about one-third of the guards who occupy the least threatening positions, the uniform style for the remainder of the new CIA guard force which carries weapons will be very similar to that worn by the White House guards and FPO officers. The uniform style consists of dark blue trousers, white long sleeve shirts, and a dark blue tie (see Attachment III). This uniform style gives an immediate improvement in appearance over the standard FPO uniform. Guard personnel assigned to the Headquarters compound will continue to wear the CIA patch which denotes Office of Security. Guards at other locations will wear nondescript patches which do not identify CIA.

CIA will assume responsibility for initial uniform issue and grant a fair allowance to each guard for replacement and cleaning. All clothing items will be returned to CIA upon termination of employment or transfer.



→ Operational Control



 TAB B

PROCEDURES RELATING TO THE COLLECTION, STORAGE AND DISSEMINATION OF INFORMATION CONCERNING THE ACTIVITIES OF UNITED STATES PERSONS

For the purpose of implementing Section 2-208 of Executive Order 12036, the Director of Central Intelligence (DCI) has established, and the Attorney General has approved, the following procedures relating to the Central Intelligence Agency's (CIA's) collection, storage and dissemination of information which is not publicly available* concerning the activities of United States persons, without the consent of such persons.

CRITERIA

1. CIA will not collect, store or disseminate information that is not available publicly concerning the activities of United States persons without their consent** unless such collection, storage and dissemination is permitted by these procedures and unless such information falls within one or more of the following categories:

a. Information concerning corporations or other commercial organizations or activities that constitutes foreign intelligence or counterintelligence, including information that (1) identifies such corporations or other commercial organizations as manufacturers of equipment or related nomenclature or (2) if deleted would hamper the correlation of information on the same subject obtained from other sources or impede the effective targeting of intelligence requirements for other sources; an organization that uses the words "Inc.," "Corp.," "Co.," "Ltd.," or other common commercial designation in its name may be presumed to be a commercial organization unless information to the contrary is obtained.

---

*Publicly available information concerning the activities of United States persons, and information of this kind that is not publicly available but that has been collected with the consent of the U.S. person concerned, may be collected, stored and disseminated whenever such information is relevant to any authorized function of CIA.

**Consent to collect implies consent to store. Dissemination of information collected pursuant to consent must meet the dissemination criteria of these procedures unless

b. Information arising out of a lawful counter-intelligence* or personnel, physical or communications security investigation, including information needed to understand or assess such investigations, information indicating that a United States person may be a target of the intelligence activities of a foreign power, or information indicating that a United States person is engaging in the unauthorized disclosure of properly classified national security information.

Counterintelligence investigations will be limited to those cases in which:

(1) facts and circumstances indicate that the person is or may be engaged in clandestine intelligence activities on behalf of a foreign power or international terrorist activity;

(2) collection is conducted to fulfill a lawful function of CIA; and

(3) collection involving use of electronic surveillance, certain surreptitious and continuous electronic or mechanical monitoring, unconsented physical searches and mail surveillance, physical surveillance and undisclosed participation in domestic organizations is conducted only in accordance with the Attorney General-approved procedures for those subjects.

Personnel security investigations involve inquiries into the activities of a person granted access to intelligence or a person to be assigned or retained in a position with sensitive duties. These investigations are designed to develop information pertaining to the suitability, eligibility and trustworthiness of the individual with respect to loyalty, character, emotional

---

consent is obtained for their dissemination. Any person or organization who solicits business from CIA or who actually engages in the provision of goods or services to CIA consents to the collection of information by CIA concerning financial or business factors which is normally collected without specific authorization by private commercial organizations which are furnished similar goods and services.

*Counterintelligence investigations within the United States can be conducted only in accordance with procedures for section 1-805 of Executive Order 12036.

stability and reliability. These investigations will be limited to collecting information about present or former CIA employees, present or former employees of CIA contractors, or applicants for such employment.

Physical security investigations involve inquiries into or surveys of the effectiveness of security controls and procedures established to protect equipment, property or classified information. Security controls and procedures include physical controls established around the perimeter of a facility, building or office; controls established with respect to the equipment or other property; procedures governing access by visitors and procedures related to access to intelligence information by persons other than employees; procedures and controls related to the safe storage and transmittal of classified information including cryptographic information, materials and equipment, procedures limiting employee access to classified information on a need-to-know basis; and procedures and controls related to the disposal of classified equipment and wastes. Physical security investigations include inquiries and other actions undertaken against United States persons who are present upon, or are in physical proximity to, an installation or facility of a CIA activity or operation and who are reasonably believed to pose a clear threat to the physical safety of personnel or property. These investigations will be limited to collecting information about persons who are:

(1) discovered in CIA premises or on a CIA installation or facility without authorization;

(2) discovered in a portion of a CIA installation or facility under such circumstances as to cause a reasonable belief that such person is violating or about to violate law or regulation relating to the protection of classified information;

(3) reasonably believed to be engaging in an activity that is directed at or will result in unauthorized entry into, or damage to a CIA installation or facility or to the security thereof; or

(4) reasonably believed to jeopardize a CIA operation or activity because of physical proximity thereto.

Communications security investigations involve inquiries into or surveys of the protective measures taken to deny unauthorized persons information derived from telecommunications.

c. Information concerning present or former employees, present or former intelligence agency contractors or their present or former employees, or applicants for any such employment or contracting, which is needed to protect foreign intelligence or counterintelligence sources or methods from unauthorzed disclosure;

d. Information needed solely to identify individuals in contact with those persons described in paragraph c immediately above or with someone who is the subject of a lawful foreign intelligence or counterintelligence investigation;

e. Information concerning persons who are reasonably believed to be potential sources or contacts, but only for the purpose of determining the suitability or credibility of such persons;

f. Information constituting foreign intelligence or counterintelligence (1) gathered abroad or (2) from electronic surveillance conducted in conformance with approved procedures or (3) from cooperating sources in the United States; cooperating sources means any organization which or individual who volunteers information or anyone who, upon being asked by anyone identifying the request as on behalf of CIA, gives the information voluntarily. "From cooperating sources" does not authorize CIA to request that a source collect information about the domestic activities of a United States person from that individual without the source revealing to that person that the source is acting on behalf of CIA.

g. Information about a person who is reasonably believed to be:

(1) acting on behalf of a foreign power;

(2) engaging in international terrorist activities;

(3) engaging in narcotics production or trafficking; or